• выбор способа настройки, наиболее удовлетворяющего профилю ИС;

• автоматическая реализация выбранного способа настройки.

Разработанный метод позволяет автоматически профилировать и настраивать произвольные информационные системы при применении политик безопасности.

В Специализированном центре защиты информации СПбГПУ разработанный метод используется в рамках практического курса «Безопасность операционных систем» для обучения принципам эффективного администрирования, грамотного применения политик безопасности, автоматизации управления безопасностью сложных вычислительных комплексов.

СПИСОК ЛИТЕРАТУРЫ:

1. *Штойер Р.* Многокритериальная оптимизация: теория, вычисления и приложения. М.: Радио и связь, 1992.
2. *Ларичев О. И.* Теория и методы принятия решений. М.: Логос, 2000.
3. *Лотов А. В., Бушенков В. А., Каменев В. А., Черных О. Л.* Компьютер и поиск компромисса. Метод достижимых целей. М.: Наука, 1997.

М. Ю. Киреев, Н. С. Шимон, Е. С. Агеев
Концерн «Созвездие», Воронеж

ПРИНЦИПЫ МОДЕЛИРОВАНИЯ МЕХАНИЗМОВ ВРЕДОНОСНОГО ВОЗДЕЙСТВИЯ НА ИНФОРМАЦИОННЫЕ ПРОЦЕССЫ В ИНТЕРЕСАХ ОЦЕНКИ УГРОЗ ИХ БЕЗОПАСНОСТИ

Формулируются основные принципы моделирования механизмов вредоносного воздействия на информационные процессы в результате противоправных действий в информационной сфере. Рассматривается возможность оценки угроз информационной безопасности, вызванных подобного рода действиями

Основополагающими гипотезами при решении задачи моделирования механизмов вредоносного воздействия на информационные процессы в интересах оценки угроз их безопасности являются гипотеза об идентифицируемости вредоносных воздействий на информационные процессы и гипотеза о многоэтапности совершения противоправных действий в информационной сфере [1].

В соответствии с первой гипотезой, несмотря на применяемые злоумышленниками способы маскирования своих противоправных действий, существуют способы идентификации вредоносных воздействий на информацию. Это дает возможность поставить в соответствие каждому вредоносному воздействию его идентифицирующие признаки, что, в свою очередь, дает возможность использовать эти признаки в качестве исходных данных для моделирования механизмов вредоносного воздействия на информационные процессы в интересах оценки угроз их безопасности.

В соответствии со второй гипотезой вредоносные воздействия реализуются в рамках многоэтапных стратегий противоправных действий. Многоэтапность этих стратегий обусловлена необходимостью преодоления (вскрытия) механизмов защиты информации.

Из приведенных гипотез вытекают основные принципы моделирования механизмов вредоносного воздействия на информационные процессы в интересах оценки угроз их безопасности.

Принцип синтеза описания противоправных действий в информационной сфере предполагает в качестве основы для формирования описаний подобного рода действий их структурный синтез.

Логически вытекающий из данного принципа принцип функционального представления противоправных действий в информационной сфере приводит к необходимости использования методов функционального моделирования для формирования описаний подобного рода действий.

В соответствии с принципом поэтапной обобщаемости признаков противоправных действий в информационной сфере оценка угроз вредоносного воздействия на информацию должна осуществляться с учетом многоэтапности стратегий подобного рода действий.

Принцип многоуровневости функционального синтеза описаний противоправных действий в информационной сфере предполагает наличие нескольких уровней функционального облика подобного рода действий.

Реализация принципа однородности описания противоправных действий в информационной сфере дает возможность описывать вредоносные воздействия на информацию такими характеристиками, через которые можно выразить все остальные их параметры как угрозу информационной безопасности. С этих позиций наиболее целесообразно использовать временные характеристики противоправных действий, так как и свойства вредоносных воздействий на информацию, и свойства средств защиты информации в общем случае зависят от времени. Кроме того, данный параметр позволяет дать количественную оценку угрозам безопасности информационных процессов.

Задачу моделирования механизмов вредоносного воздействия на информационные процессы в интересах оценки угроз их безопасности на основе сформулированных признаков целесообразно решать путем представления в виде следующих основных последовательно решаемых задач:

- структуризация описаний противоправных действий в информационной сфере в интересах оценки угроз информационной безопасности;
- унификация методов моделирования механизмов вредоносного воздействия на информационные процессы в интересах оценки угроз их безопасности с целью получения номенклатуры моделей, не превышающей заданной;
- проведение экспериментов по определению возможности оценки угроз безопасности информационных процессов.

СПИСОК ЛИТЕРАТУРЫ:

1. Правовое обеспечение информационной безопасности: учебник для высших учебных заведений МВД России / В. А. Минаев, А. П. Фисун, С. В. Скрыль, С. В. Дворянкин, М. М. Никитин, Н. С. Хохлов. М.: Маросейка, 2008. – 368 с.